

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10015520-1

IN THE  
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Julie SYMONS et al.

Confirmation No.: 9441

Application No.: 10/005,066

Examiner: Tran, N.V.

Filing Date: December 3, 2001

Group Art Unit: 2151

Title: METHOD FOR DETECTING AND PREVENTING INTRUSION IN A VIRTUALLY-WIRED SWITCHING FABRIC

Mail Stop Appeal Brief-Patents  
Commissioner For Patents  
PO Box 1450  
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 5/9/2007.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month  
\$120

☐ 2nd Month  
\$450

☐ 3rd Month  
\$1020

☐ 4th Month  
\$1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:  
Commissioner for Patents, Alexandria, VA 22313-1450  
Date of Deposit:

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile: 7/9/2007

Typed Name: Ilene Fish

Signature: 

Respectfully submitted,

Julie SYMONS et al.

By 

John P. Wagner, Jr.

Attorney/Agent for Applicant(s)

Reg No.: 35,398

Date: 07/09/2007

Telephone: 408-377-0500



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant: SYMONS, et al. Patent Application  
Application No.: 10/005,066 Group Art Unit: 2151  
Filed: December 03, 2001 Examiner: Tran, N. V.  
For: METHOD FOR DETECTING AND PREVENTING INTRUSION IN A  
VIRTUALLY-WIRED SWITCHING FABRIC

APPEAL BRIEF

07/13/2007 RFEKADU1 00000024 082025 10005066  
01 FC:1402 500.00 DA

HP-10015520-1  
Serial No.: 10/005,066

Group Art Unit: 2151



## Table of Contents

	<u>Page</u>
Real Party in Interest	1
Related Appeals and Interferences	2
Status of Claims	3
Status of Amendments	4
Summary of Claimed Subject Matter	5
Grounds of Rejection to Be Reviewed on Appeal	9
Argument	10
Conclusion	20
Appendix – Clean Copy of Claims on Appeal	21
Appendix – Evidence Appendix	26
Appendix – Related Proceedings Appendix	27



I. Real Party in Interest

The assignee of the present invention is Hewlett-Packard Development Company,

L.P.

HP-10015520-1  
Serial No.: 10/005,066

Group Art Unit: 2151

## II. Related Appeals and Interferences

The instant application (10/005,066) is a continuation-in-part of application number 09/971,857, "Method and System for Describing and Comparing Data Center Physical and Logical Topologies and Device Configurations." Both applications share the same two inventors and are commonly assigned to the real party in interest, Hewlett-Packard Development Company, L.P. An appeal for Application Number 09/971,857 was filed on June 11, 2007, and was stamped as received by the Office of Initial Patent Examination on June 14, 2007. The appeal for Application Number 09/971,857 is pending, and thus no decision on this matter has yet been received by the Appellants.

### III. Status of Claims

Claims 1-12 and 23 have previously been cancelled. Claims 13-22 and 24-38 remain pending. Claims 13-22 and 24-38 are rejected. This Appeal involves Claims 13-22 and 24-38.

#### IV. Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

## V. Summary of Claimed Subject Matter

Independent Claims 13, 22, and 31 of the present application pertain to embodiments associated with a network and methods for managing a network.

Claim 13 recites, “a computer-readable medium having stored thereon a program, which when run on a processor, performs a method of managing a network.” This embodiment is depicted in flowchart 400 of Figure 5 and described from page 15, line 16 to page 17, line 14 of the specification and additionally on page 9, lines 13-13 of the specification. For example, “a computer-readable medium may have instructions stored thereon, which when run on a processor, perform steps of process 400,” is described (page 15, lines 15-19).

With reference to flowchart 400, “comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses,” is illustrated in steps 410, 420, 430, and 440. As shown in flowchart 400, “[i]n step 410, the management system 220 reads the database 210 to obtain a list of interconnect ports 125” (page 15, lines 19-21). “Next, in step 420, the management system 220 reads the database 210 to obtain a list of expected MAC addresses based on the topology. In this fashion, the management system 220 may determine the authorized MAC addresses that are expected to be present in the network 100,” (page 15, line 23 - page 16, line 2). “In step 430, a bridge table is read to determine which MAC addresses were learned at interconnect port 125...[f]or clarity, process 400 is described as processing one interconnect port 125 at a time and looping back from step 480 to step 430, until all interconnect ports 125 have been processed,” (page 16, lines 4-10). “In step 440, the management system 220 determines if a MAC address in the bridge table is on the expected list of MAC addresses for this interconnect port 125,” (page 16, lines 14-16). As described on page 9, lines 14-18, “[t]his monitoring compares the MAC addresses that each interconnect port 125 ‘learns’ (e.g., MAC addresses that are associated with packets processed at an interconnect port 125) with a



set of MAC addresses that are expected to be seen at that interconnect port 125, based on the network topology.”

With reference to flowchart 400, “tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network” is shown in 450. For example, “[i]f the MAC address is not expected, then the topology is traced by reading bridge tables of other switches 120 to find the host port 115 where the unexpected MAC address was learned, in step 450.” Additionally, as described on page 9, lines 18-21, “[i]f an unexpected MAC address is seen, this embodiment may trace the topology to find the host port 115 where the unexpected MAC address was ‘learned’ (e.g., where the packet entered the virtually-wired switching fabric 250).”

Claim 22 recites, “[a] method of managing a network.” This embodiment is depicted in: process 300 (illustrated in Figure 3), process 345 (illustrated in Figure 4), and step 450 of flowchart 400 (illustrated in Figure 5). Description of process 300 appears on page 13, line 7 to page 14, line 11 of the specification. Description of process 345 appears on page 14, line 13 to page 15, line 14 of the specification. Description of step 450 appears on page 16, line 21 - page 17, line 2 of the specification.

“[A]ccessing a database of a stored physical topology of said network to obtain authorized addresses at host ports of switches,” is described in step 310, where, “...a database 210 is read to obtain a list of expected MAC addresses at each host port 115,” (page 13, lines 10-12). “[C]onfiguring a switch in said network to forward a packet received at a first port if an address associated with said packet is authorized for said first port,” is described in step 320, where, “... port host filters are added based on the expected MAC addresses or addresses at each host port 115,” (page 14, lines 1 - 2). “For example, the management system 220 instructs the configuration agent 230 to add host port filters by configuring the switches 120,” (page 14, lines 2-4).

“[C]omparing a set of learned addresses against a set of expected addresses, said learned addresses comprising addresses associated with packets processed at a second port, said expected addresses derived from an expected configuration of said network” is described in step 340 of process 345. “In step 340, the MAC address associated with the packet is compared to a list of expected MAC addresses for this host port 115,” page 14, lines 21-22. “[T]racing a topology of said network to find a third port where an unexpected address entered said network, said third port coupled to a device having a media access control (MAC address) that is said unexpected address,” is described in Claim 23 (page 30, lines 6-9) of the specification as filed, and is also described in conjunction with step 450 of flowchart 400 (page 16, line 21 to page 17, line 2).

Claim 31 recites, “[a] network.” This network is described in conjunction with Figures 1 and 2. “Figure 1 is a diagram of a physical environment (e.g., network) 100 with a virtually-wired switching fabric 250,” (page 6, lines 11-13). As recited in Claim 31, “a plurality of switches,” is shown in Figure 1 (virtually wired switching fabric 250 is comprised of a plurality of switches 120). As recited in Claim 31, the switches 120 are “interconnected and configured to control communication between a plurality of devices coupled to said network,” page 6, line 15 to page 7, line 10).

As recited in Claim 31, “a database having stored therein a stored physical topology of said network and authorized addresses associated with packets processed at ports of said switches, wherein said authorized addresses are based on said stored physical topology,” is illustrated in item 210 of Figure 2. The database is described at least on page 10, line 25 to page 11, line 4 and on page 13, lines 10-24. As recited in Claim 31, “a configuration agent that is able to program said switches based on said authorized addresses to detect a packet having an unauthorized address,” is illustrated in item 230 of Figure 2 and described at least on page 11, lines 15-18 and also on page 14, lines 2-8). As recited in Claim 31, “a

management agent that is able to: compare addresses learned by said switches against said authorized addresses to determine an unauthorized address; and trace a topology of said network to determine a port where a packet associated with said unauthorized address entered said network,” is shown in item 220 (management system) of Figure 2. These particular characteristics of management system 220 are described at least on page 15, line 19 to page 17, line 2 of the specification.

## VI. Grounds of Rejection to Be Reviewed on Appeal

Claims 13-16, 18-20, and 25-30 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0083344 to Vairavan in view of U.S. Patent No. 6,538,997 to Wang et al. (hereinafter Wang).

Claims 17 and 24 are rejected under are rejected under 35 U.S.C. §103(a) 35 U.S.C. §103(a) as being unpatentable over Vairavan in view of Wang, and further in view of U.S. Patent No. 5,805,801 to Holloway et al. (hereinafter Holloway).

Claims 31-38 are rejected under are rejected under 35 U.S.C. §103(a) 35 U.S.C. §103(a) as being unpatentable over Vairavan in view of Wang, and further in view of Holloway.

The Rejection characterizes Appellants' arguments as improper for arguing individually against a particular element that each prior Art reference has the same deficiency with regard to the particular element. Appellants view this characterization of their arguments as improper and wish to appeal it.

## VII. Argument

### 1. Whether Claims 13-16, 18-21, and 25-30 are unpatentable under 35 U.S.C. §103(a) by Vairavan in view of Wang.

Claim 13 that recites that an embodiment of the present invention is directed to (emphasis added):

A computer-readable medium having stored thereon a program, which when run on a processor, performs a method of managing a network, said method comprising:

comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses; and

tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network.

Independent Claim 22 recites similar limitations. Claims 14-16 and 18-21 that depend from Independent Claim 13 and Claims 25-30 that depend from Independent Claim 22 provide further recitations of the features of the present invention.

A. The cited references do not meet the claim limitation of “comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses,” (emphasis added).

Appellants respectfully submit that Vairavan does not teach, suggest, or describe, “comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses,” as claimed (emphasis added). Instead, Appellants understand Vairavan to teach a networking device including a packet processor that can function as a network address translation (NAT) router (page 4-5, para. 60 of Vairavan). The packet processor can also include a firewall module for providing security based on a security policy database (page 6, para. 86 of Vairavan). Appellants understand the firewall module to implement different types of filtering algorithms for restricting access within a virtual private network (VPN) (page 6, para. 86 - page 7, para. 101). The Examiner contends in the Response to Arguments section (page 12, part 28 of the office action dated 02/09/2007) that this claim limitation is taught by Vairavan: “For example the firewall module 310 analyzes, isolates, filters, and discards packets (page 6,

para. 86 of Vairavan). Analyzing, isolating, filtering, and discarding packets is an example of comparing addresses to determine unexpected addresses.”

Appellants disagree with this contention and the Rejection’s characterization of “filtering” as taught by Vairavan. Specifically, Appellants submit that the firewall module of Vairavan is not operable for “comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses,” as claimed (emphasis added). Instead, per Appellants’ understanding, Vairavan may teach filtering based upon source and destination addresses of a packet (page 6, paragraphs 74 and 80 of Vairavan); “content filtering of packets” (page 6, para. 88); “...stateful inspection of a packet to identify states that the packet has completed” (page 7, para. 89); and “...a network intrusion detection mechanism that monitors packet packets transmitted to or from specific device...” for “...anomaly detection and misuse detection,” (page 7, para. 90). However, while Vairavan may refer to some certain kinds of filtering, Appellants submit that Vairavan does not teach, suggest, or describe, “comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses,” as claimed (emphasis added) and as contended by the Examiner.

Furthermore, Appellants respectfully assert that the combination of Vairavan and Wang fails to teach or suggest this claimed embodiment because Wang does not overcome the shortcomings of Vairavan. Appellants have reviewed the Wang reference and have found no teaching that, alone or in combination with Vairavan, teaches or suggests the limitation of “comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses,” as claimed (emphasis added).

Therefore, Appellants respectfully submit that the Examiner's rejection of Claims 13-16, 18-21, and 25-30 does not satisfy the requirements of a *prima facie* case of obviousness as claim limitations are not met by the cited references. As such, Appellants submit that Claims 13 and 22 overcome the rejection under 35 U.S.C. §103(a), and are thus in a condition for allowance. Moreover, Appellants respectfully submit that Claims 14-16, 18-21, and 25-30 also overcome the rejection under 35 U.S.C. §103(a), and are in a condition for allowance as being dependent on allowable base claims.

B. The cited references do not meet the claim limitation of "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added).

The Rejection of 02/09/07 states, "... Vairavan does not explicitly show tracing a topology of said network to find a third port where an unexpected address entered said network, said third port coupled to a device having a media access control (MAC address) that is said unexpected address," (first full paragraph of page 3). Appellants agree and further assert that Vairavan does not teach, describe, or suggest the limitation of, "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added).

Furthermore, Appellants respectfully assert that the combination of Vairavan and Wang fails to teach or suggest the claimed embodiments because Wang does not overcome the shortcomings of Vairavan. Appellants submit that Wang, alone or in combination with Vairavan, does not show or suggest either "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added). Instead, per Appellants' understanding, the Wang reference is silent in regard this limitation and therefore does not cure this deficiency of Vairavan.

The Rejection of 02/09/2007 contends that Wang teaches this limitation in col. 1, lines 11-32 and col. 5, line 9 - col. 6, line 65 (see second full paragraph on page 3 of the Rejection). Appellants disagree with this contention. Instead, Appellants understand Wang to teach that a layer-2 trace can be used "... to gather general information related to the switched network, or to gather specific diagnostic information relating to a particular path through the switched network," (col. 6, lines 18-21 of Wang). Further, per Appellants' understanding, the traces taught by Wang are utilized to: isolate or receive switch configuration information, to isolate frame loss problems, to trace a path between a sender and receiver, to discover information such as the maximum transmit units of a path, or to diagnose a problem with a specific path. See, e.g., col. 5, line 13 - col. 6, line 65 of Wang. Per Appellants' understanding, the above described "tracing" performed by Wang is for determining network efficiencies or diagnosing a communications problem, such as troubleshooting a path when a problem or fault occurs in the transmission of packets within the network (see., e.g., col. 1, lines 11-32 of Wang).

Appellants submit that Wang's "tracing" for such troubleshooting purposes is very different than, and does not teach or suggest, "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added). As such, Appellants submit that the Wang reference, either alone or in combination with Vairavan, does not teach or suggest this claim limitation.

Therefore, for this additional reason, Appellants respectfully submit that the Examiner's rejection of Claims 13-16, 18-21, and 25-30 does not satisfy the requirements of a *prima facie* case of obviousness as claim limitations are not met by the cited references. Further, Appellants submit that the invention as recited in Claims 13 and 22 would not be obvious to one of ordinary skill in the art at the time based upon the cited combinations discussed above (as was generally alleged in the Response to Arguments section, part 31, page 13 of the Office Action of 02/09/2007). As such, Appellants submit that Claims 13 and



22 overcome the rejection under 35 U.S.C. §103(a), and are thus in a condition for allowance. Moreover, Appellants respectfully submit that Claims 14-16, 18-21, and 25-30 also overcome the rejection under 35 U.S.C. §103(a), and are in a condition for allowance as being dependent on allowable base claims.

2. Whether Claims 17 and 24 are unpatentable under 35 U.S.C. §103(a) by Vairavan in view of Wang and further in view of Holloway.

The Rejection of 02/09/07 states, "... Vairavan does not explicitly show tracing a topology of said network to find a third port where an unexpected address entered said network, said third port coupled to a device having a media access control (MAC address) that is said unexpected address," (first full paragraph on page 3). Appellants agree and further assert that Vairavan does not teach, describe, or suggest the limitation of, "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added).

Furthermore, Appellants respectfully assert that the combination of Vairavan and Wang fails to teach or suggest the claimed embodiments because Wang does not overcome the shortcomings of Vairavan. Appellants submit that Wang, alone or in combination with Vairavan, does not show or suggest either "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added). Instead, per Appellants' understanding, the Wang reference is silent in regard this limitation and therefore does not cure this deficiency of Vairavan.

The Rejection of 02/09/2007 contends that Wang teaches this limitation in col. 1, lines 11-32 and col. 5, line 9 - col. 6, line 65 (see second full paragraph on page 3 of the Rejection). Appellants disagree with this contention. Instead, Appellants understand Wang to teach that a layer-2 trace can be used "... to gather general information related to the

switched network, or to gather specific diagnostic information relating to a particular path through the switched network,” (col. 6, lines 18-21 of Wang). Further, per Appellants’ understanding, the traces taught by Wang are utilized to: isolate or receive switch configuration information, to isolate frame loss problems, to trace a path between a sender and receiver, to discover information such as the maximum transmit units of a path, or to diagnose a problem with a specific path. See, e.g., col. 5, line 13 - col. 6, line 65 of Wang. Per Appellants’ understanding, the above described “tracing” performed by Wang is for determining network efficiencies or diagnosing a communications problem, such as troubleshooting a path when a problem or fault occurs in the transmission of packets within the network (see., e.g., col. 1, lines 11-32 of Wang).

Appellants submit that Wang’s “tracing” for such troubleshooting purposes is very different than, and does not teach or suggest, “tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network,” as claimed (emphasis added). As such, Appellants submit that the Wang reference, either alone or in combination with Vairavan, does not teach or suggest this claim limitation.

Appellants submit that the Holloway reference does not cure this deficiency of the combination of the Vairavan reference in view of the Wang reference. Namely, per Appellants’ understanding, the Holloway reference is silent with respect to any sort of tracing of a network topology, let alone “tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network,” as recited in Claim13 and similarly in Claim 22 (emphasis added).

As such, Appellants submit that the Holloway reference, either alone or in combination with Vairavan in view of Wang, does not teach or suggest the claim limitation of, “tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network,” as recited in Claim13 and similarly in Claim 22.

Further, Appellants submit that the invention as recited in Claims 13 and 22 would not be obvious to one of ordinary skill in the art at the time based upon the cited combinations discussed above (as was generally alleged in the Response to Arguments section, part 31, page 13 of the Office Action of 02/09/2007). Therefore, Appellants submit the Claims 13 and 22 are allowable over the combination of Vairavan in view of Wang and further in view of Holloway. Moreover, Appellants respectfully submit that Claims 17 and 24 also overcome the rejection under 35 U.S.C. §103(a), and are in a condition for allowance as being dependent on allowable independent Claims 13 and 22.

3. Whether Claims 31-38 are unpatentable under 35 U.S.C. §103(a) by Vairavan in view of Wang and further in view of Holloway.

Claim 31 that recites that an embodiment of the present invention is directed to  
(emphasis added):

A network comprising:  
a plurality switches;  
said switches interconnected and configured to control  
communication between a plurality of devices coupled to said network;  
a database having stored therein a stored physical topology of said  
network and authorized addresses associated with packets processed at  
ports of said switches, wherein said authorized addresses are based on said  
stored physical topology;  
a configuration agent that is able to program said switches based  
on said authorized addresses to detect a packet having an unauthorized  
address; and  
a management agent that is able to:  
compare addresses learned by said switches against said  
authorized addresses to determine an unauthorized address; and  
trace a topology of said network to determine a port where  
a packet associated with said unauthorized address entered said  
network.

Claims 32-38 that depend from Independent Claim 31 provide further recitations of the features of the present invention.

The Rejection of 02/09/2007 does not rely upon the Vairavan reference to teach or suggest the limitation of, “a management agent that is able to...trace a topology of said

network to determine a port where a packet associated with said unauthorized address entered said network,” as is recited in Claim 31. Further, Appellants submit that the Vairavan reference does not teach or suggest this limitation.

The Rejection of 02/09/07 contends that the Wang reference suggests or discloses, “tracing a topology of said network [i.e. tracing of the computer network, col. 1, lns 11-32, and col.5, ln. 98- col. 6, ln. 65] to find a third port where an unexpected address entered said network, said third port coupled to a device having a media access control (MAC address),” (see Rejection, page 8, first full paragraph). The (page 8, second full paragraph) contends that,

... it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Vairavan in view of Wang by tracing a topology of said network to find a third port where an unexpected address entered said network, said third port coupled to a device having a media access control (MAC address) that is said unexpected address because this feature is a consequence of the topologies being aligned [Wang, col. 6, lns. 63-65].

Appellants disagree with the Rejection’s characterization of the Wang reference as teaching this limitation. Instead, Appellants submit that Wang, alone or in combination with Vairavan, does not teach or suggest, “a management agent that is able to ... trace a topology of said network to determine a port where a packet associated with said unauthorized address entered said network,” as claimed (emphasis added).

Appellants understand Wang to teach that a layer-2 trace can be used “... to gather general information related to the switched network, or to gather specific diagnostic information relating to a particular path through the switched network,” (col. 6, lines 18-21 of Wang). Further, per Appellants’ understanding, the traces taught by Wang are utilized to isolate or receive switch configuration information, to isolate frame loss problems, to trace a path between a sender and receiver, to discover information such as the maximum transmit units of a path, or to diagnose a problem with a specific path. See, e.g., col. 5, line 13 - col. 6,

line 65 of Wang. Per Appellants' understanding, the above described "tracing" performed by Wang is for determining network efficiencies or diagnosing a communications problem, such as troubleshooting a path when a problem or fault occurs in the transmission of packets within the network (see., e.g., col. 1, lines 11-32).

Appellants submit that Wang's "tracing" for such troubleshooting purposes is very different than, and does not teach or suggest, "a management agent that is able to ... trace a topology of said network to determine a port where a packet associated with said unauthorized address entered said network," as claimed (emphasis added). As such, Appellants submit that the Wang reference, either alone or in combination with Vairavan, does not teach or suggest this claim limitation.

Appellants submit that the Holloway reference does not cure this deficiency of the combination of the Vairavan reference in view of the Wang reference. Namely, per Appellants' understanding, the Holloway reference is silent with respect to any sort of tracing of a network topology, let alone "a management agent that is able to ... trace a topology of said network to determine a port where a packet associated with said unauthorized address entered said network," as recited in Claim 31 (emphasis added). Thus, Appellants submit that this limitation of Claim 31 is not taught or suggested by the combination of Vairavan in view of Wang and further in View of Holloway.

Therefore, for this reason, Appellants respectfully submit that the Examiner's rejection of Claim 31 does not satisfy the requirements of a *prima facie* case of obviousness as claim limitations are not met by the cited references. Further, Appellants submit that the invention as recited in Claim 31 would not be obvious to one of ordinary skill in the art at the time based upon the cited combinations discussed above (as was generally alleged in the Response to Arguments section, part 31, page 13 of the Office Action of 02/09/2007). As such, Appellants submit that Claim 31 overcomes the rejection under 35 U.S.C. §103(a), and

is thus in a condition for allowance. Moreover, Appellants respectfully submit that Claims 32-38 also overcome the rejection under 35 U.S.C. §103(a), and are in a condition for allowance as being dependent on allowable independent Claim 31.

4. Whether the Appellants' arguments are improper for arguing individually against a particular element that each prior Art reference has the same deficiency with regard to the particular element.

On page 13, part 30 of the Rejection of 02/09/2007, the following is stated:

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking reference individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Applicant obviously attacks references individually without taking into consideration based on the teaching of combinations of references as shown in the above.

It is respectfully submitted that the definition of improperly arguing references individually would be to argue claim limitation 1 of Claim A on the basis of one reference and then to argue claim limitation 2 of Claim A on the basis of a second reference. Appellants submit that was not done.

An example of a proper response would be to argue claim limitation 1 of Claim A on the basis of one reference and then to argue claim limitation 1 of Claim A on the basis of a second reference, thus showing that neither reference taught or suggested claim limitation 1. Appellants submit that the Arguments provided herein (and in the previous Office Action responses) take such form, and thus are proper. Therefore, it is respectfully submitted that responses previously provided to the Examiner were not improper due to their method of argument, and were thus in proper form for argument against a 35 U.S.C. §103 rejection.

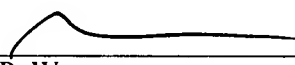
Conclusion

Appellants believe that pending Claims 13-22 and 24-38 are patentable over the cited combinations of the Vairavan, Wang, and Holloway references. As such, Appellants submit that Claims 13-22 and 24-38 are patentable over the prior art.

Appellants respectfully request that the rejection of Claims 13-22 and 24-38 be reversed. The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellants' undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,  
WAGNER BLECHER LLP

Dated: 7/9, 2007

  
\_\_\_\_\_  
John P. Wagner  
Registration No. 35,398  
123 Westridge Drive  
Watsonville, CA 95076  
San Jose, CA 95113

Phone: (408) 377-0500  
Facsimile: (408) 722-2350

VIII. Appendix - Clean Copy of Claims on Appeal

13. (Previously Presented) A computer-readable medium having stored thereon a program, which when run on a processor, performs a method of managing a network, said method comprising:

comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses; and

tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network.

14. (Original) The computer-readable medium of Claim 13 wherein said network is a virtually-wired switching network and said first port couples switches in said network and said second port is coupled to a host device.

15. (Previously Presented) The computer-readable medium of Claim 13, wherein said network comprises a virtually-wired switching fabric.

16. (Previously Presented) The computer-readable medium of Claim 15, wherein said method further comprises:

taking corrective action at said second port, wherein said second port is coupled to a host device.

17. (Previously Presented) The computer-readable medium of Claim 15, wherein said method further comprises:

disabling said second port, wherein said second port is at the edge of said virtually-wired switching fabric.



18. (Previously Presented) The computer-readable medium of Claim 13 wherein said comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses comprises reading a bridge table to determine learned addresses at said first port.

19. (Previously Presented) The computer-readable medium of Claim 13 wherein said comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses is repeated for each interconnect port in said network, wherein said network comprises a plurality of switches.

20. (Previously Presented) The computer-readable medium of Claim 13, wherein said method further comprises:

determining changes in physical topology of said network.

21. (Previously Presented) The computer-readable medium of Claim 20 wherein said determining changes in physical topology of said network comprises comparing a physical description of said network with a stored physical description of said network.

22. (Previously Presented) A method of managing a network, said method comprising:

accessing a database of a stored physical topology of said network to obtain authorized addresses at host ports of switches;

configuring a switch in said network to forward a packet received at a first port if an address associated with said packet is authorized for said first port;

comparing a set of learned addresses against a set of expected addresses, said learned addresses comprising addresses associated with packets processed at a second port, said expected addresses derived from an expected configuration of said network; and

tracing a topology of said network to find a third port where an unexpected address entered said network, said third port coupled to a device having a media access control (MAC address) that is said unexpected address.

24. (Previously Presented) The method of Claim 22, further comprising:  
disabling said third port, wherein said network is a virtually-wired switching fabric and said third port is at the edge of said virtually-wired switching fabric.

25. (Previously Presented) The method of Claim 22, wherein said configuring the switch further comprises configuring the switch to drop said packet if said address is not authorized.

26. (Previously Presented) The method of Claim 22, wherein said configuring the switch comprises programming the switch in said network to recognize authorized addresses for said first port.

27. (Previously Presented) The method of Claim 22, wherein said configuring the switch further comprises configuring the switch to forward said packet to a host device if said address is authorized for said first port, said first port coupled to said host device.

28. (Previously Presented) The method of Claim 22, further comprising:  
determining changes in physical topology of said network.

29. (Previously Presented) The method Claim 28 wherein said determining changes in physical topology comprises comparing a physical description of said network with said stored physical topology of said network.

30. (Original) The method of Claim 29 wherein said address is a media access control (MAC) address and wherein said network comprises a virtually-wired switching fabric.

31. (Previously Presented) A network comprising:  
a plurality switches;  
said switches interconnected and configured to control communication between a plurality of devices coupled to said network;  
a database having stored therein a stored physical topology of said network and authorized addresses associated with packets processed at ports of said switches, wherein said authorized addresses are based on said stored physical topology;  
a configuration agent that is able to program said switches based on said authorized addresses to detect a packet having an unauthorized address; and  
a management agent that is able to:  
compare addresses learned by said switches against said authorized addresses to determine an unauthorized address; and  
trace a topology of said network to determine a port where a packet associated with said unauthorized address entered said network.

32. (Previously Presented) The network of Claim 31, wherein:  
said switches are further configured to forward said packet if said address is authorized.

33. (Previously Presented) The network of Claim 31, wherein:  
said switches are further configured to drop said packet if said address is not authorized.

34. (Original) The network of Claim 31, wherein there is a one-to-one mapping between ports of said switches and ports of said devices.

35. (Previously Presented) A network as recited in Claim 31 wherein said addresses are medium control access (MAC) addresses.

36. (Previously Presented) A network as recited in Claim 31 wherein said network comprises a virtually-wired switching fabric.

37. (Previously Presented) A network as recited in Claim 31 wherein said management agent is further able to determine changes in said physical topology of said network and to update said stored physical topology and authorized addresses in said database based on said changes.

38. (Previously Presented) A network as recited in Claim 37 wherein said configuration agent is further able to re-program said switches based on said updates to said authorized addresses.

IX. Evidence Appendix

No evidence is herein appended.

#### X. Related Proceedings Appendix

No decisions have been rendered by a Court or the Board of Patent Appeals and Interferences in the related appeal proceeding for Application Number 09/971,857 which is listed in Section II of this Appeal Brief. As such, there is no decision on this matter which the Appellants can include in this Appendix.